UNITED STATES DISTRICT COURT

for the

Western District of Washington

In the Matter of the Search of *(Briefly describe the property to be searched or identify the person by name and address)* 510 Sky Country Way NW, Issaquah, Washington 98027, as further described in Attachment A	)	Case No. MJ20-270

APPLICATION FOR A SEARCH WARRANT

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property *(identify the person or describe the property to be searched and give its location):*

See Attachment A

located in the Western District of Washington, there is now concealed *(identify the person or describe the property to be seized)*:

See Attachment B

The basis for the search under Fed. R. Crim. P. 41(c) is *(check one or more)*:

- ☑ evidence of a crime;
- ☑ contraband, fruits of crime, or other items illegally possessed;
- ☑ property designed for use, intended for use, or used in committing a crime;
- ☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section	*Offense Description*
18 USC Sections 1343, 1344	Wire Fraud, Bank Fraud

The application is based on these facts:

✓ See Affidavit of Special Agent Cole Ashcraft continued on the attached sheet.

☐ Delayed notice of days (give exact ending date if more than 30 days:) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

Pursuant to Fed. R. Crim. P. 4.1, this warrant is presented: ☑ by reliable electronic means; or: ☐ telephonically recorded.

Cole Ashcraft

Applicant's signature

Cole Ashcraft, Special Agent, TIGTA

Printed name and title

◯ The foregoing affidavit was sworn to before me and signed in my presence, or

◉ The above-named agent provided a sworn statement attesting to the truth of the foregoing affidavit by telephone.

Date: 05/21/2020

Judge's signature

City and state: Seattle, Washington

Mary Alice Theiler, United States Magistrate Judge

Printed name and title

USAO: 2020R00487

AFFIDAVIT

STATE OF WASHINGTON)
) ss
COUNTY OF KING)

I, Cole Ashcraft**,** having been duly sworn, state as follows:

INTRODUCTION AND AGENT BACKGROUND

1. I am a Special Agent with the Treasury Inspector General for Tax Administration (TIGTA) and have been since December 2019. Prior to that, I was a Special Agent with the U.S. Postal Service Office of Inspector General since 2013 and was assigned to their Computer Crimes Unit for the majority of that time. I have received formal training in both computer science and the investigation of computer crimes, including network intrusions and computer forensics. I have investigated or assisted in the investigation of numerous cases involving fraudulent activity in connection with computers. I am currently assigned to TIGTA's Cybercrime Investigations Division and the FBI Washington Field Office Cyber Task Force. I investigate violations of federal laws regarding the programs and operations of the Internal Revenue Service (IRS) and Federal tax administration. I have been a sworn law enforcement officer during all times herein.

2. I make this affidavit in support of an application under Rule 41 of the Federal Rules of Criminal Procedure for a warrant to search the premises located at 510 Sky Country Way NW, Issaquah, Washington, 98027, hereinafter "SUBJECT PREMISES," as more fully described in Attachment A to this Affidavit, for the property and items described in Attachment B to this Affidavit, as well as any digital devices or other electronic storage media located therein.

3. The facts set forth in this Affidavit are based on my own personal knowledge; knowledge obtained from other individuals during my participation in this investigation, including other law enforcement officers; interviews of cooperating witnesses; review of documents and records related to this investigation; communications with others who have

UNITED STATES ATTORNEY
700 STEWART ST, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

personal knowledge of the events and circumstances described herein; and information gained through my training and experience.

4. Because this Affidavit is submitted for the limited purpose of establishing probable cause in support of the application for a search warrant, it does not set forth each and every fact that I or others have learned during the course of this investigation. I have set forth only the facts that I believe are necessary to establish probable cause to believe that evidence, fruits and instrumentalities of violations of 18 U.S.C. § 1343 (Wire Fraud), 18 U.S.C. § 1344 (Bank Fraud), 18 U.S.C. § 1014 (False Statements to a Financial Institution), and 15 U.S.C. § 645(a) (False Statements to the Small Business Administration) will be found at the SUBJECT PREMISES.

THE INVESTIGATION

The Paycheck Protection Program

5. The Coronavirus Aid, Relief, and Economic Security ("CARES") Act is a federal law enacted in or around March 2020 and designed to provide emergency financial assistance to the millions of Americans who are suffering the economic effects caused by the COVID-19 pandemic. One source of relief provided by the CARES Act was the authorization of up to $349 billion in forgivable loans to small businesses for job retention and certain other expenses, through a program referred to as the Paycheck Protection Program ("PPP"). In or around April 2020, Congress authorized over $300 billion in additional PPP funding.

6. In order to obtain a PPP loan, a qualifying business must submit a PPP loan application, which is signed by an authorized representative of the business. The PPP loan application requires the business (through its authorized representative) to acknowledge the program rules and make certain affirmative certifications in order to be eligible to obtain the PPP loan. In the PPP loan application, the small business (through its authorized representative) must state, among other things, its: (a) average monthly payroll expenses; and (b) number of employees. These figures are used to calculate the amount of money

UNITED STATES ATTORNEY
700 STEWART ST, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

the small business is eligible to receive under the PPP. In addition, businesses applying for a PPP loan must provide documentation showing their payroll expenses.

7. A PPP loan application must be processed by a participating financial institution (the lender). If a PPP loan application is approved, the participating financial institution funds the PPP loan using its own monies, which are 100% guaranteed by Small Business Administration (SBA). Data from the application, including information about the borrower, the total amount of the loan, and the listed number of employees, is transmitted by the lender to the SBA in the course of processing the loan.

8. PPP loan proceeds must be used by the business on certain permissible expenses—payroll costs, interest on mortgages, rent, and utilities. The PPP allows the interest and principal on the PPP loan to be entirely forgiven if the business spends the loan proceeds on these expense items within a designated period of time (usually eight weeks of receiving the proceeds) and uses at least 75% of the PPP loan proceeds on payroll expenses.

Baoke Zhang and Related Entities

9. Baoke Zhang is a legal permanent resident of the United States and holds a valid Chinese passport. According to information obtained in the investigation, Zhang resides at the SUBJECT PREMISES. A publicly available LinkedIn profile believed to be Zhang's states that Zhang is a software engineer working at Lyft, Inc., a ridesharing company headquartered in San Francisco, California.

10. Records from Comcast Communications LLC, an internet service provider, show that an IP address, 24.22.166.81, ("the Zhang IP address") is subscribed to Zhang at the SUBJECT PREMISES. According to IRS records, it is the same IP address that has been used to access Zhang's personal tax information on IRS websites since 2017

11. According to records obtained from the IRS, an Employer Identification Number ("EIN") was applied for and assigned to a sole proprietorship in Zhang's name, Baoke Zhang dba Baoke Zhang, ("the Zhang sole proprietorship"), on or about April 3,

UNITED STATES ATTORNEY
700 STEWART ST, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

2020. According to IRS records, the EIN was applied for and obtained from the Zhang IP address registered to the SUBJECT PREMISES.

a. According to records from the Washington State Department of Revenue ("DOR"), a business license was applied for in the name of the Zhang sole proprietorship on or about April 8, 2020. The license was issued on or about April 17, 2020. The application lists Zhang as the owner of the business, the SUBJECT PREMISES as the business address, and 310-408-3314 as the business phone number. It also reports $0 to $12,000 in estimated annual income in Washington State, reports no employees in the city in where the business is located, and claims to have been in operation in Washington State since in or about November 2017. According to information obtained from the Washington State Economic Security Department ("ESD"), the state agency with which businesses register for the purpose of employer-paid state unemployment tax and paid leave benefits, the agency has no record of the Zhang sole proprietorship.

b. DOR has provided the government copies of letters addressed to Zhang at the SUBJECT PREMISES about the sole proprietorship's tax obligations dated on or about April 13, 2020.

12. According to records obtained from the IRS, an EIN was applied for and assigned to an entity named Cloud Optimization LLC ("Cloud Optimization") on or about April 21, 2020. According to IRS and internet service provider records, the Zhang IP address, subscribed to the SUBJECT PREMISES, was used to obtain the EIN. According to records and information obtained from the Washington State Secretary of State ("SOS"), ESD, and DOR, the agencies have no record of Cloud Optimization.

PPP Loan Applications Submitted for the Zhang Sole Proprietorship and Cloud Optimization

13. The government has obtained copies of three applications for PPP loans totaling more than $1.5 million that each bear a signature in Zhang's name and were submitted to two SBA-approved lenders in or about April 2020. The applications were

UNITED STATES ATTORNEY
700 STEWART ST, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

submitted to the lenders from the Zhang IP address registered to the SUBJECT PREMISES.

14. One application was submitted on behalf of the Zhang sole proprietorship to Ready Capital, a publicly traded real estate investment trust with its primary offices in New York, Texas, and New Jersey, that participates in the SBA's PPP loan program as an SBA Preferred Lender. A Preferred Lender is a lender that's been pre-approved by the SBA to accept applications for, underwrite, and disburse SBA loans with little to no SBA involvement. These lenders have demonstrated their proficiency in SBA guaranteed loan programs and processes.

15. Two additional applications were submitted to PayPal, which forwarded the applications to WebBank, an FDIC-insured, state-charted industrial bank headquartered in Salt Lake City, Utah, that is an approved SBA lender, for funding. One application was submitted in the name of the Zhang sole proprietorship and one was submitted in the name of Cloud Optimization. According to information obtained from a PayPal representative, PayPal collects all PPP loan application documents and reviews them. Once the application package is complete, the applicant digitally signs the package and it is forwarded to WebBank, the actual lender. The servers that initially accept the loan documentation from the applicant are located in Oregon.

16. The applications sought loans in the following amounts for the following entities:

Entity Name	Lender	Loan Amount	Approximate Date of Application
Baoke Zhang dba Baoke Zhang	Ready Capital	$600,000	April 10, 2020
Baoke Zhang dba Baoke Zhang	PayPal/WebBank	$600,000	April 19, 2020
Cloud Optimization	PayPal/WebBank	$325,000	April 23, 2020

17. Each application identified Zhang as the "Primary Contact" and 100 percent owner of the entity listed on the relevant application. Each application also identified

UNITED STATES ATTORNEY
700 STEWART ST, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

Zhang by his social security number and the address of the SUBJECT PREMISES. A copy of a Washington State driver's license in Zhang's name and with his identifying information, including the address of the SUBJECT PREMISES, also was submitted with each application.

18. Financial records, public records, and phone records obtained during the investigation show that each of the applications submitted under Zhang's name included multiple materially false statements about the eligibility of each of the entities for PPP loans. Specifically, while each application and records provided in support of it purported to claim and show that the entities had been in business as of February 15, 2020, and had paid employees—requirements for eligibility—each entity actually was created in or about April 2020 and had no identifiable employment expenses. In addition, evidence obtained in the investigation demonstrates that digital devices using the Zhang IP address registered to the SUBJECT PREMISES were used in the course of the scheme to submit fraudulent PPP loan applications.

Fraudulent PPP Loan Application Submitted to Ready Capital for the Zhang Sole Proprietorship

19. According to records provided by Ready Capital, Zhang digitally signed an application package in support of a $600,000 PPP loan for the Zhang sole proprietorship and submitted it to Ready Capital from the Zhang IP address registered to the SUBJECT PREMISES on or about April 10, 2020.

20. Ready Capital provided the government the SBA Form 2483 submitted with the package and bearing the signature of Zhang. To support the loan amount, the application represented that the sole proprietorship had an average monthly payroll of $240,000 and 25 employees. Zhang also certified that the sole proprietorship "was in operation on February 15, 2020 and has employees for whom it paid salaries and payroll taxes or paid independent contractors." As described further herein, evidence obtained in the investigation demonstrates that this certification was false.

UNITED STATES ATTORNEY
700 STEWART ST, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

21. Ready Capital has provided several documents it received in support of the application, including purported IRS records and a purported payroll detail report from an online payroll system. A review of those documents and records and information obtained from the IRS and ESD demonstrate that the documents provided to Ready Capital were falsified and included materially false statements about the sole proprietorship's operations.

a. An IRS Notice CP 575, which notifies applicants of the assignment of an EIN, was submitted with the application package. The CP 575 submitted to Ready Capital stated that the EIN for the Zhang sole proprietorship, 85-0611741, was assigned on April 3, 2017. As described above, that EIN was actually obtained using the Zhang IP address registered to the SUBJECT PREMISES on or about April 3, 2020. The EIN was assigned by the Modernized Internet EIN application (MODIEIN)—an application on the IRS website that allows businesses to apply for EINs online. The IRS includes a timestamp in the file names of MODIEIN-generated Notice CP 575s. The file name of the electronic copy of the Notice CP 575 provided to Ready Capital included this timestamp. The timestamp reflects the notice was issued on April 3, 2020, not in 2017 as represented. The submitted Notice CP 575 file also lacked certain technical data encoded in MODIEIN-generated Notice CP 575s, indicating it was not a genuine notice or had been modified after being downloaded from MODIEIN. The metadata of the modified Notice also indicated it had been produced using an Apple Inc. operating system, noted as macOS. MODIEIN does not run under macOS. Records from the IRS also show that the Zhang IP address registered to the SUBJECT PREMISES was used to access information about obtaining an EIN on or about April 2, 2020, and April 3, 2020.

b. An IRS Form 941, an Employer's Quarterly Federal Tax Return, was submitted with the application package purporting to report wages and federal payroll tax information for the sole proprietorship for the fourth quarter of 2019. According to the form, the Zhang sole proprietorship had 25 employees in the fourth quarter and paid wages, tips, and total compensation totaling $717,560.38. The form also appears to have

UNITED STATES ATTORNEY
700 STEWART ST, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

a handwritten signature in Zhang's name and a handwritten date of January 3, 2020. Based on a search of available IRS records related to the EIN associated with the Zhang sole proprietorship, no such IRS Form 941 has been submitted to the IRS. Records from the IRS demonstrate that the Zhang IP address registered to the SUBJECT PREMISES was used to access information about Form 941 on or about April 2, 2020, and April 3, 2020, and to download the same edition of the Form 941 submitted to Ready Capital on or about April 8, 2020.

c. A Form 1040 with attachments, signed with Zhang's signature and dated on or about March 3, 2020, was submitted with the application package purporting to be Zhang's personal income tax return for 2019. Included in the attachments was a Schedule C, which reports profits and losses of a sole proprietorship. The Schedule C purported to report approximately $138,700 in profit in 2019 for the Zhang sole proprietorship. Based on a search of available IRS records related to Zhang and the EIN associated with the Zhang sole proprietorship, no such Schedule C has been submitted to the IRS. According to metadata in the electronic file submitted to Ready Capital, the Form 1040 and attachments were created on or about April 9, 2020, using software believed to have been released by Intuit Inc. on or about March 27, 2020. According to records from the IRS, the Zhang IP address registered to the SUBJECT PREMISES was used to access information about and download a Schedule C on or about April 9, 2020 and April 29, 2020.

d. A document purporting to be a record from an online payroll system was submitted with the application package listing payroll detail records for 25 employees for calendar year 2019. According to the document submitted, the Zhang sole proprietorship incurred more than approximately $2.8 million in payroll in 2019. According to the document, expenses for many employees included payments for "WA SUI" and "WA PFML ER." Based on publicly available information, "WA SUI" is believed to refer to Washington State unemployment tax payments and "WA PFML ER" is believed to refer to Washington State paid family medical leave benefits. As described

UNITED STATES ATTORNEY
700 STEWART ST, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

above, ESD, the Washington State agency that maintains records of such payments, has no record of the Zhang sole proprietorship.

22. In addition to the records provided in support of the loan application, Ready Capital has provided email correspondence with resortwatsons@gmail.com, the email address listed on the application it received. The individual using the account identified himself in correspondence as "Baoke" and used the account to make additional false statements to Ready Capital in support of the application.

a. On or about May 4, 2020, a representative of Knight Capital Funding, Ready Capital's underwriter for the application, emailed resortwatsons@gmail.com and stated, in part:

> Good morning, Baoke, . . . There's a discrepancy in some information we hope you could clear up for us: The SBA records show your EIN ending 1741 was established 4/3/2020[.] However, the 2019 Tax information provided (returns, 941's) shows the same EIN ending 1741 already in use last year. Would you be able to explain the discrepancy between these two dates? When was this EIN actually established? Please provide your SS4 from the IRS showing the date the EIN was established. Please reply by 5PM EST today, or we will have to decline your file.

b. Later the same day, a response sent from resortwatsons@gmail.com and signed by "Baoke" stated in part:

> Good morning. Thank you so much for reaching out. I am sorry to forget keeping Ready Capital update. There are some change in situation with my business in last a few days, and don't need this loan. I would like to withdraw and cancel my ppp loan application. Could you help cancel my loan application with SBA? So the loan can be available to other small business who urgently need it. Regarding the SBA EIN number, I don't know why SBA record incorrectly show the date. My business and EIN date back to 2017. Please see attached SS4. Again thank you and ready capital for assistance during the process. I have declined the loan doc. Thank you and have a nice day.

UNITED STATES ATTORNEY
700 STEWART ST, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

An IRS Notice CP 575 was attached to the email which purported to show that the EIN for the Zhang sole proprietorship was issued on April 3, 2017. As described above, this document was falsified.

23. Based on the discrepancy in the records and the response it received in the email correspondence with resortwatsons@gmail.com, Ready Capital never approved the PPP loan to the Zhang sole proprietorship.

Fraudulent PPP Loan Application Submitted to PayPal and WebBank for the Zhang Sole Proprietorship

24. According to records provided by PayPal, Zhang digitally signed an application package in support of a $600,000 PPP loan for his sole proprietorship and submitted it to PayPal from the Zhang IP address registered to the SUBJECT PREMISES on or about April 19, 2020.

25. PayPal provided the government the SBA Form 2483 submitted with the package and bearing the signature of Zhang. To support the loan amount, the application represented that the sole proprietorship had an average monthly payroll of $240,000 and 25 employees. Zhang also certified that the sole proprietorship "was in operation on February 15, 2020 and has employees for whom it paid salaries and payroll taxes or paid independent contractors." As described further herein, evidence obtained in the investigation demonstrates that this certification was false.

26. PayPal also provided the government a loan agreement signed in Zhang's name on or about April 19, 2020, between Zhang and WebBank. The loan agreement identified WebBank as the lender and an FDIC-insured institution and included a certification by Zhang that the information related to the application was complete and correct. As described further herein, evidence obtained in the investigation demonstrates that this certification was false.

27. PayPal has provided several documents it received in support of the application for the Zhang sole proprietorship. Most of them are the same false documents provided to Ready Capital described above, including the falsified CP 575

UNITED STATES ATTORNEY
700 STEWART ST, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

purporting to show the entity's EIN was issued in 2017, the falsified Form 941 for the fourth quarter of 2019, the false Schedule C, and the payroll detail report purporting to show payments of Washington State unemployment taxes and paid leave benefits in 2019 of which ESD has no record. According to records from PayPal, digital file copies of these records were submitted in support of the loan application on or about April 16, 2020.

28. In addition, PayPal has provided documents it received in support of the application that were not part of the application package provided by Ready Capital in relation to the first loan application for the Zhang sole proprietorship. According to records from PayPal, digital file copies of these records were submitted in support of the loan application on or about April 14 and April 16, 2020. A review of records and information from the IRS, ESD, and DOR show that these too were falsified and contained false statements.

a. Additional Forms 941, for the first three quarters of 2019, were submitted with the application package purporting to show the entity had 25 employees for which it paid wages, tips, and compensation in each quarter. Based on a search of available IRS records related to the EIN associated with the Zhang sole proprietorship, no such Forms 941 have been submitted to the IRS. IRS records show that after the first submission to Ready Capital, the Zhang IP address registered to the SUBJECT PREMISES was used to access information about and download Forms 941 again on or about April 8, 2020.

b. The loan application package included what purported to be a payroll detail report from an online payroll system for 2020 showing the payment of Washington State unemployment taxes and paid leave benefits for many employees. As described above, according to information obtained from ESD, it has no record of the entity ever having registered or made such payments.

c. The loan application packaged included an electronic document purporting to be from the Washington State Business Licensing Service stating that the Zhang sole proprietorship's business license had been renewed on or about February 8,

UNITED STATES ATTORNEY
700 STEWART ST, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

2020. As described above, records from DOR show that the Zhang sole proprietorship first applied for a business license on or about April 8, 2020.

29. After WebBank learned of the government's investigation, it did not fund the loan.

Fraudulent PPP Loan Application Submitted to PayPal and WebBank for Cloud Optimization

30. According to records provided by PayPal, Zhang digitally signed an application package in support of a $325,000 PPP loan for Cloud Optimization and submitted it to PayPal from the Zhang IP address registered to the SUBJECT PREMISES on or about April 23, 2020.

31. PayPal provided the government the SBA Form 2483 submitted with the package and bearing the signature of Zhang. To support the loan amount, the application represented that the sole proprietorship had an average monthly payroll of $130,000 and 20 employees. Zhang also certified that Cloud Optimization "was in operation on February 15, 2020 and has employees for whom it paid salaries and payroll taxes or paid independent contractors." As described further herein, evidence obtained in the investigation demonstrates that this certification was false.

32. PayPal also provided the government a loan agreement signed in Zhang's name on or about April 23, 2020, between Zhang and WebBank. The loan agreement identified WebBank as the lender and an FDIC-insured institution and included a certification by Zhang that the information related to the application was complete and correct. As described further herein, evidence obtained in the investigation demonstrates that this certification was false.

33. PayPal has provided several documents it received in support of the application, including purported IRS records, Washington State records, and payroll detail reports from an online payroll platform. According to records provided by PayPal, digital file copies of these records were submitted on or about April 23, 2020. A review of those documents and records and information obtained from the IRS, DOR, ESD, SOS, and Bank

UNITED STATES ATTORNEY
700 STEWART ST, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

of America demonstrate that the documents provided to PayPal were falsified and included materially false statements about Cloud Optimization's operations.

a. The submitted application package included an IRS Notice CP 575 purporting to show that the EIN for Cloud Optimization, 85-0782607, was assigned on April 21, 2018. As described above, IRS records demonstrate that the EIN was actually assigned on April 21, 2020, not 2018, and was applied for and obtained from the Zhang IP address registered to the SUBJECT PREMISESs. Technical data encoded in the submitted Notice CP 575 file indicate the file was created on April 21, 2020, and modified on April 22, 2020.

b. The submitted application package included IRS Forms 941 purporting to report wages and federal payroll tax information for Cloud Optimization for each quarter of calendar year 2019. According to the forms, Cloud Optimization had 20 employees in each quarter and paid approximately $394,000 to $396,000 in quarterly wages, tips, and compensation. Based on a search of available IRS records related to the EIN associated with Cloud Optimization, no such IRS Forms 941 have been submitted to the IRS.

c. The submitted application package included an electronic document purporting to be an electronic copy of a publicly available record from DOR's online business information database. According to the document provided, a business license was first issued to Cloud Optimization on or about February 8, 2018, and the entity was assigned Unique Business Identifier (UBI) number 604-601-873. Information obtained from DOR and SOS reflects that no entity named Cloud Optimization has ever been registered with the state of Washington and the UBI listed on the document does not exist.

d. The submitted application package included electronic documents purporting to be records from an online payroll platform listing payroll detail records for 20 employees for calendar year 2019 and the first quarter of 2020. According to the documents submitted, Cloud Optimization incurred more than approximately $1.5 million in payroll in 2019 and more than approximately $397,128 in payroll in 2020. According

UNITED STATES ATTORNEY
700 STEWART ST, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

to the documents, expenses for many employees included payments for "WA SUI" and "WA PFML EE." Based on publicly available information, "WA SUI" is believed to refer to Washington State unemployment tax payments and "WA PFML EE" is believed to refer to Washington State paid family medical leave benefits. As described above, ESD has informed the government that it has no record of Cloud Optimization registering with the agency or making any such payments.

e. The submitted application package included an electronic document purporting to be a Bank of America statement for the period December 7, 2019, to January 8, 2020, for an account ending in 5806 in the names of Zhang and Cloud Optimization. The record purported to show 20 separate payments to the 20 individuals listed on the payroll records provided. Records from Bank of America show that the account ending in 5806 was established in or about April 2020 in the name of "Baoke Zhang dba Baoke Zhang," with Zhang as the sole signatory. Records from the account show no payments to anyone matching those on the fake account statement submitted to PayPal.

34. WebBank approved the Cloud Optimization loan application on or about May 3, 2020. On or about May 5, 2020, WebBank attempted to transmit the $325,000 in approved funds to the account ending in 5806. On or about May 6, 2020, the money was returned before it was deposited because the account name did not match that provided to WebBank. After WebBank learned of the government's investigation, it did not fund the loan.

Use of Digital Devices to Carry Out the Fraud from the SUBJECT PREMISES

35. Information obtained during the investigation demonstrates that digital devices accessing the Internet from the Zhang IP address registered to the SUBJECT PREMISES were used to carry out the above-described wire fraud and bank fraud schemes.

36. From at least in or about April 2, 2020 to at least in or about May 6, 2020, the Zhang IP address subscribed to the SUBJECT PREMISES was used to access IRS websites and obtain IRS forms and information relevant to the fraudulent applications. For example, on or about April 2, 2020, April 3, 2020 (the same day an EIN was applied for

UNITED STATES ATTORNEY
700 STEWART ST, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

and obtained for the Zhang sole proprietorship), and April 8, 2020, the Zhang IP address was used to access the landing page for the MODIEIN application, access information about filing Forms 941 and 944 (Employer's Annual Federal Tax Return), and downloaded copies of Forms 940 (Employer's Annual Federal Unemployment Tax Return), 941, and 944. The Zhang IP address also was used during that time to access the FAQ page for "Does a small company that operates as a sole proprietorship need an employer identification number (EIN)?"

37. According to IRS records, at least two Apple, Inc., devices, a MacBook and an iPhone, have been used to access IRS websites from the SUBJECT PREMISES during the above-described time period.

38. In addition, as described above, several IRS Forms downloaded using the Zhang IP address registered to the SUBJECT PREMISES are the same IRS Forms for which falsely completed copies were later provided to lenders in support of the above-described fraudulent loan applications. For example, on or about April 8, 2020, the Zhang IP address registered to the SUBJECT PREMISES was used to download copies of IRS Form 941. The metadata for the Form 941 submitted on behalf of the Zhang sole proprietorship to Ready Capital indicates the "Author" is "Baoke Zhang" and the document was created on or about April 9, 2020, using an Apple, Inc. device operating system.

39. The Zhang IP address registered to the SUBJECT PREMISES also was used to submit certified and signed copies of each of the above-described applications to Ready Capital and PayPal.

Recorded Calls and Records from T-Mobile Phone Number
Associated with the Businesses Located at SUBJECT PREMISES

40. The phone number 310-408-3314 is listed as the business phone number for the Zhang sole proprietorship and Cloud Optimization on each of the loan applications and on the sole proprietorship's application for a Washington State business license, all of which also identify the SUBJECT PREMISES as the entities' business location. It is also

UNITED STATES ATTORNEY
700 STEWART ST, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

listed a Zhang's contact information on the publicly available LinkedIn profile believed to belong to Zhang.

41. Subscriber records obtained from T-Mobile show that the number was activated on or about March 22, 2019, and is associated with the brand Ultra. According to publicly available information, Ultra provides pre-paid phone services using T-Mobile's network. There is no other subscriber data associated with the number.

42. On or about May 7, 2020, after the wire to Cloud Optimization was returned, the phone records for 310-408-3314 show an approximately 2.5 minute call with a toll free number associated with Swift Financial, a subsidiary of PayPal. PayPal has provided an approximately 2.5 minute recorded call on or about May 7, 2020, between a PayPal representative and a male individual identifying himself on the call as "Baoke." On the call, after the PayPal representative asked Zhang to provide a voided check or bank statement to confirm the account to which the wire should be sent, the individual first stated he no longer wanted the loan and then stated he would discuss it with "the team."

43. On or about May 12, 2020, a recorded call was made with an individual identifying himself as "Baoke" who was using 310-408-3314. The individual refused to answer additional identification verification questions about himself. The individual confirmed that he had two loan applications outstanding with PayPal for the Zhang sole proprietorship and Cloud Optimization for $600,000 and $325,000, respectively, and stated he no longer needed the loans. The individual stated that he had conferred with his "legal team" and they did not feel comfortable disclosing the reason the entities no longer needed the loans. No evidence gathered in the investigation to date suggests that any attorneys or any other individuals are involved in any operations of the Zhang sole proprietorship or Cloud Optimization.

44. Based on a lay comparison of the voices of the individual identifying himself as "Baoke" on the May 7 and May 12 calls, it appears that the same male voice was speaking on both calls.

UNITED STATES ATTORNEY
700 STEWART ST, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

Surveillance of the SUBJECT PREMISES

45. On or about May 14, 2020, Federal Bureau of Investigation special agents conducted surveillance of the SUBJECT PREMISES. The property is a single-family home. The agents observed a male matching Zhang's height and race and wearing glasses in the driveway of the SUBJECT PREMISES and eventually entering the SUBJECT PREMISES. According to driver's license records, Zhang wears corrective lenses. Agents attempted to call 310-408-3314 while the male individual was in view, but the call went to voicemail. The male was not observed reaching for a cell phone or attempting to answer a call. He did, however, disappear from view on the west side of the SUBJECT PREMISES during part of the attempted call.

TECHNICAL TERMS

46. Based on my training and experience, I use the following technical terms to convey the following meanings:

a. IP Address: The Internet Protocol address (or simply "IP address") is a unique numeric address used by computers on the Internet. An IP address looks like a series of four numbers, each in the range 0-255, separated by periods (e.g., 121.56.97.178). Every digital device attached to the Internet must be assigned an IP address so that Internet traffic sent from and directed to that digital device may be directed properly from its source to its destination. Most Internet service providers control a range of IP addresses. Some computers have static-that is, long-term-IP addresses, while other computers have dynamic-that is, frequently changed-IP addresses.

b. Internet: The Internet is a global network of computers and other electronic devices that communicate with each other. Due to the structure of the Internet, connections between devices on the Internet often cross state and international borders, even when the devices communicating with each other are in the same state.

c. Electronic Storage media: Electronic Storage media is any physical object upon which data can be recorded. Examples include hard disks, RAM, floppy disks, flash memory, CD-ROMs, and other magnetic or optical media.

COMPUTERS, ELECTRONIC STORAGE, AND FORENSIC ANALYSIS

47. As described above and in Attachment B, this application seeks permission to search for evidence, fruits, and/or instrumentalities that might be found at the SUBJECT

UNITED STATES ATTORNEY
700 STEWART ST, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

PREMISES, in whatever form they are found. One form in which the evidence, fruits, and instrumentalities might be found is data stored on digital devices[1] such as computer hard drives or other electronic storage media.[2] Thus, the warrant applied for would authorize the seizure of digital devices or other electronic storage media or, potentially, the copying of electronically stored information from digital devices or other electronic storage media, all under Rule 41(e)(2)(B).

48. *Probable cause.* Based upon my review of the evidence gathered in this investigation, my review of data and records, information received from other agents and computer forensics examiners, and my training and experience, I submit that if a digital device or other electronic storage media is found at the SUBJECT PREMISES, there is probable cause to believe that evidence, fruits, and/or instrumentalities of violations of 18 U.S.C. § 1343 (Wire Fraud), 18 U.S.C. § 1344 (Bank Fraud), 18 U.S.C. § 1014 (False Statements to a Financial Institution), and 15 U.S.C. § 645(a) (False Statements to the Small Business Administration) will be stored on those digital devices or other electronic storage media. Based on my review of IRS data and metadata in the electronic files submitted to the lenders described above, I believe digital devices or other electronic storage media are being used to access the Internet using the Zhang IP address registered to the SUBJECT PREMISES to review and download IRS information and forms later used to support fraudulent PPP loan applications. I also believe that digital devices and

---

[1] "Digital device" includes any device capable of processing and/or storing data in electronic form, including, but not limited to: central processing units, laptop, desktop, notebook or tablet computers, computer servers, peripheral input/output devices such as keyboards, printers, scanners, plotters, monitors, and drives intended for removable media, related communications devices such as modems, routers and switches, and electronic/digital security devices, wireless communication devices such as mobile or cellular telephones and telephone paging devices, personal data assistants ("PDAs"), iPods/iPads, Blackberries, digital cameras, digital gaming devices, global positioning satellite devices (GPS), or portable media players.

[2] Electronic Storage media is any physical object upon which electronically stored information can be recorded. Examples include hard disks, RAM, floppy disks, flash memory, CD-ROMs, and other magnetic or optical media.

UNITED STATES ATTORNEY
700 STEWART ST, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

other electronic storage media are being used to alter electronic documents or create false electronic documents and submit them, by accessing the Internet using the Zhang IP address registered to the SUBJECT PREMISES, to lenders in support of fraudulent PPP loan applications. There is, therefore, probable cause to believe that evidence, fruits and/or instrumentalities of violations of 18 U.S.C. § 1343 (Wire Fraud), 18 U.S.C. § 1344 (Bank Fraud), 18 U.S.C. § 1014 (False Statements to a Financial Institution), and 15 U.S.C. § 645(a) (False Statements to the Small Business Administration) exists and will be found on digital device or other electronic storage media at the SUBJECT PREMISES, for at least the following reasons:

a. Based on my knowledge, training, and experience, I know that computer files or remnants of such files can be preserved (and consequently also then recovered) for months or even years after they have been downloaded onto a storage medium, deleted, or accessed or viewed via the Internet. Electronic files downloaded to a digital device or other electronic storage medium can be stored for years at little or no cost. Even when files have been deleted, they can be recovered months or years later using forensic tools. This is so because when a person "deletes" a file on a digital device or other electronic storage media, the data contained in the file does not actually disappear; rather, that data remains on the storage medium until it is overwritten by new data.

b. Therefore, deleted files, or remnants of deleted files, may reside in free space or slack space—that is, in space on the digital device or other electronic storage medium that is not currently being used by an active file—for long periods of time before they are overwritten. In addition, a computer's operating system may also keep a record of deleted data in a "swap" or "recovery" file.

c. Wholly apart from user-generated files, computer storage media—in particular, computers' internal hard drives—contain electronic evidence of how a computer has been used, what it has been used for, and who has used it. To give a few examples, this forensic evidence can take the form of operating system configurations, artifacts from operating system or application operation; file system data structures, and virtual memory "swap" or paging files. Computer users typically do not erase or delete this evidence, because special software is typically required for that task. However, it is technically possible to delete this information.

UNITED STATES ATTORNEY
700 STEWART ST, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

d. Similarly, files that have been viewed via the Internet are sometimes automatically downloaded into a temporary Internet directory or "cache."

49. Based on actual inspection of the IRS forms, payroll detail reports, and other electronic documents submitted in support of the above-described fraudulent loan applications, I am aware that digital devices and other electronic storage media were used to generate, store, and print documents used in the fraud scheme.

50. *Forensic evidence.* As further described in Attachment B, this application seeks permission to locate not only computer files that might serve as direct evidence of the crimes described on the warrant, but also for forensic electronic evidence that establishes how digital devices or other electronic storage media were used, the purpose of their use, who used them, and when. There is probable cause to believe that this forensic electronic evidence will be on any digital devices or other electronic storage media located at the SUBJECT PREMISES because:

a. Stored data can provide evidence of a file that was once on the digital device or other electronic storage media but has since been deleted or edited, or of a deleted portion of a file (such as a paragraph that has been deleted from a word processing file). Virtual memory paging systems can leave traces of information on the digital device or other electronic storage media that show what tasks and processes were recently active. Web browsers, e-mail programs, and chat programs store configuration information that can reveal information such as online nicknames and passwords. Operating systems can record additional information, such as the history of connections to other computers, the attachment of peripherals, the attachment of USB flash storage devices or other external storage media, and the times the digital device or other electronic storage media was in use. Computer file systems can record information about the dates files were created and the sequence in which they were created.

b. As explained herein, information stored within a computer and other electronic storage media may provide crucial evidence of the "who, what, why, when, where, and how" of the criminal conduct under investigation, thus enabling the United States to establish and prove each element or alternatively, to exclude the innocent from further suspicion. In my training and experience, information stored within a computer or storage media (e.g., registry information, communications, images and movies, transactional information, records of session times and durations, internet history, and anti-virus, spyware, and malware detection programs) can indicate who has used or controlled the

UNITED STATES ATTORNEY
700 STEWART ST, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

computer or storage media. This "user attribution" evidence is analogous to the search for "indicia of occupancy" while executing a search warrant at a residence. The existence or absence of anti-virus, spyware, and malware detection programs may indicate whether the computer was remotely accessed, thus inculpating or exculpating the computer owner and/or others with direct physical access to the computer. Further, computer and storage media activity can indicate how and when the computer or storage media was accessed or used. For example, as described herein, computers typically contain information that log: computer user account session times and durations, computer activity associated with user accounts, electronic storage media that connected with the computer, and the IP addresses through which the computer accessed networks and the internet. Such information allows investigators to understand the chronological context of computer or electronic storage media access, use, and events relating to the crime under investigation.[1] Additionally, some information stored within a computer or electronic storage media may provide crucial evidence relating to the physical location of other evidence and the suspect. For example, images stored on a computer may both show a particular location and have geolocation information incorporated into its file data. Such file data typically also contains information indicating when the file or image was created. The existence of such image files, along with external device connection logs, may also indicate the presence of additional electronic storage media (e.g., a digital camera or cellular phone with an incorporated camera). The geographic and timeline information described herein may either inculpate or exculpate the computer user. Last, information stored within a computer may provide relevant insight into the computer user's state of mind as it relates to the offense under investigation. For example, information within the computer may indicate the owner's motive and intent to commit a crime (e.g., internet searches indicating criminal planning), or consciousness of guilt (e.g., running a "wiping" program to destroy evidence on the computer or password protecting/encrypting such evidence in an effort to conceal it from law enforcement).

c. A person with appropriate familiarity with how a digital device or other electronic storage media works can, after examining this forensic evidence in its

[1] For example, if the examination of a computer shows that: a) at 11:00am, someone using the computer used an internet browser to log into a bank account in the name of John Doe; b) at 11:02am the internet browser was used to download child pornography; and c) at 11:05 am the internet browser was used to log into a social media account in the name of John Doe, an investigator may reasonably draw an inference that John Doe downloaded child pornography.

UNITED STATES ATTORNEY
700 STEWART ST, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

proper context, draw conclusions about how the digital device or other electronic storage media were used, the purpose of their use, who used them, and when.

d. The process of identifying the exact files, blocks, registry entries, logs, or other forms of forensic evidence on a digital device or other electronic storage media that are necessary to draw an accurate conclusion is a dynamic process. While it is possible to specify in advance the records to be sought, digital evidence is not always data that can be merely reviewed by a review team and passed along to investigators. Whether data stored on a computer is evidence may depend on other information stored on the computer and the application of knowledge about how a computer behaves. Therefore, contextual information necessary to understand other evidence also falls within the scope of the warrant.

e. Further, in finding evidence of how a digital device or other electronic storage media was used, the purpose of its use, who used it, and when, sometimes it is necessary to establish that a particular thing is not present. For example, the presence or absence of counter-forensic programs or anti-virus programs (and associated data) may be relevant to establishing the user's intent.

PAST EFFORTS TO OBTAIN ELECTRONICALLY STORED INFORMATION

51. I know that on or about May 12, 2020, the U.S. District Court for the District of Columbia issued a search warrant to search the two Google LLC ("Google") email accounts listed as the contact addresses for the Zhang sole proprietorship and Cloud Optimization—resortwatsons@gmail.com and cloudoptimizationllc@gmail.com, respectively. In addition, I know that, on or about May 15, 2020, the U.S. District Court for the District of Columbia issued an Order pursuant to 18 U.S.C. § 2703(d) for various subscriber and user activity associated with a Google email account believed to be Zhang's personal email account. Google has not yet complied with either the search warrant or the Order. While the warrant I apply for today would allow seizure of information on digital devices at the SUBJECT PREMISES that may also have been attached to emails contained in the Google accounts or otherwise stored in the Google accounts, the warrant I apply for today would allow seizure of additional information not likely to be in those accounts, such as IRS forms downloaded locally on a digital device before provision to a lender.

52. Because of the nature of the evidence that I am attempting to obtain and the nature of the investigation, I have not made any further efforts to obtain the evidence based

UNITED STATES ATTORNEY
700 STEWART ST, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

on the consent of any party who may have authority to consent. I believe, based upon the nature of the investigation and the information I have received, that if Zhang becomes aware of the investigation in advance of the execution of a search warrant, he may attempt to destroy any potential evidence, whether digital or non-digital, thereby hindering law enforcement agents from the furtherance of the criminal investigation.

RISK OF DESTRUCTION OF EVIDENCE

53. I know based on my training and experience that digital information can be very fragile and easily destroyed. Digital information can also be easily encrypted or obfuscated such that review of the evidence would be extremely difficult, and in some cases impossible. In the instant case, I know based on information gathered in the investigation that Zhang has experience as a software engineer and thus likely has extensive knowledge of the ways in which digital information can be destroyed or encrypted. If an encrypted computer is either powered off or if the user has not entered the encryption password and logged onto the computer, it is likely that any information contained on the computer will be impossible to decipher. If the computer is powered on, however, and the user is already logged onto the computer, there is a much greater chance that the digital information can be extracted from the computer. This is because when the computer is on and in use, the password has already been entered and the data on the computer is accessible. However, giving the owner of the computer time to activate a digital security measure, pull the power cord from the computer, or even log off of the computer could result in a loss of digital information that could otherwise have been extracted from the computer.

REQUEST FOR AUTHORITY TO CONDUCT OFF-SITE SEARCH OF TARGET COMPUTERS

54. *Necessity of seizing or copying entire computers or storage media.* In most cases, a thorough search of premises for information that might be stored on digital devices or other electronic storage media often requires the seizure of the physical items and later off-site review consistent with the warrant. In lieu of removing all of these items from the

UNITED STATES ATTORNEY
700 STEWART ST, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

premises, it is sometimes possible to make an image copy of the data on the digital devices or other electronic storage media, onsite. Generally speaking, imaging is the taking of a complete electronic picture of the device's data, including all hidden sectors and deleted files. Either seizure or imaging is often necessary to ensure the accuracy and completeness of data recorded on the item, and to prevent the loss of the data either from accidental or intentional destruction. This is true because of the following:

a. *The time required for an examination*. As noted above, not all evidence takes the form of documents and files that can be easily viewed on site. Analyzing evidence of how a computer has been used, what it has been used for, and who has used it requires considerable time, and taking that much time on premises could be unreasonable. As explained above, because the warrant calls for forensic electronic evidence, it is exceedingly likely that it will be necessary to thoroughly examine the respective digital device and/or electronic storage media to obtain evidence. Computer hard drives, digital devices and electronic storage media can store a large volume of information. Reviewing that information for things described in the warrant can take weeks or months, depending on the volume of data stored, and would be impractical and invasive to attempt on-site.

b. *Technical requirements*. Digital devices or other electronic storage media can be configured in several different ways, featuring a variety of different operating systems, application software, and configurations. Therefore, searching them sometimes requires tools or knowledge that might not be present on the search site. The vast array of computer hardware and software available makes it difficult to know before a search what tools or knowledge will be required to analyze the system and its data on the premises. However, taking the items off-site and reviewing them in a controlled environment will allow examination with the proper tools and knowledge.

c. *Variety of forms of electronic media*. Records sought under this warrant could be stored in a variety of electronic storage media formats and on a variety of digital devices that may require off-site reviewing with specialized forensic tools.

SEARCH TECHNIQUES

55. Based on the foregoing, and consistent with Rule 41(e)(2)(B) of the Federal Rules of Criminal Procedure, the warrant I am applying for will permit seizing, imaging, or otherwise copying digital devices or other electronic storage media that reasonably appear capable of containing some or all of the data or items that fall within the scope of

UNITED STATES ATTORNEY
700 STEWART ST, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

Attachment B to this Affidavit, and will specifically authorize a later review of the media or information consistent with the warrant.

56. Because several people share the SUBJECT PREMISES as a residence, it is possible that the SUBJECT PREMISES will contain digital devices or other electronic storage media that are predominantly used, and perhaps owned, by persons who are not suspected of a crime. If agents conducting the search nonetheless determine that it is possible that the things described in this warrant could be found on those computers, this application seeks permission to search and if necessary to seize those computers as well. It may be impossible to determine, on scene, which computers contain the things described in this warrant.

57. Consistent with the above, I hereby request the Court's permission to seize and/or obtain a forensic image of digital devices or other electronic storage media that reasonably appear capable of containing data or items that fall within the scope of Attachment B to this Affidavit, and to conduct off-site searches of the digital devices or other electronic storage media and/or forensic images, using the following procedures:

A. Processing the Search Sites and Securing the Data.

a. Upon securing the physical search site, the search team will conduct an initial review of any digital devices or other electronic storage media located at the subject premises described in Attachment A that are capable of containing data or items that fall within the scope of Attachment B to this Affidavit, to determine if it is possible to secure the data contained on these devices onsite in a reasonable amount of time and without jeopardizing the ability to accurately preserve the data.

b. In order to examine the electronically stored information ("ESI") in a forensically sound manner, law enforcement personnel with appropriate expertise will attempt to produce a complete forensic image, if possible and appropriate, of any digital device or other electronic storage media that is capable of containing data or items that fall within the scope of Attachment B to this Affidavit.[1]

[1] The purpose of using specially trained computer forensic examiners to conduct the imaging of digital devices or other electronic storage media is to ensure the integrity of the evidence and to follow proper, forensically sound, scientific procedures. When the

UNITED STATES ATTORNEY
700 STEWART ST, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

c. A forensic image may be created of either a physical drive or a logical drive. A physical drive is the actual physical hard drive that may be found in a typical computer. When law enforcement creates a forensic image of a physical drive, the image will contain every bit and byte on the physical drive. A logical drive, also known as a partition, is a dedicated area on a physical drive that may have a drive letter assigned (for example the c: and d: drives on a computer that actually contains only one physical hard drive). Therefore, creating an image of a logical drive does not include every bit and byte on the physical drive. Law enforcement will only create an image of physical or logical drives physically present on or within the subject device. Creating an image of the devices located at the search locations described in Attachment A will not result in access to any data physically located elsewhere. However, digital devices or other electronic storage media at the search locations described in Attachment A that have previously connected to devices at other locations may contain data from those other locations.

d. If based on their training and experience, and the resources available to them at the search site, the search team determines it is not practical to make an on-site image within a reasonable amount of time and without jeopardizing the ability to accurately preserve the data, then the digital devices or other electronic storage media will be seized and transported to an appropriate law enforcement laboratory to be forensically imaged and reviewed.

B. Searching the Forensic Images.

a. Searching the forensic images for the items described in Attachment B may require a range of data analysis techniques. In some cases, it is possible for agents and analysts to conduct carefully targeted searches that can locate evidence without requiring a time-consuming manual search through unrelated materials that may be commingled with criminal evidence. In other cases, however, such techniques may not yield the evidence described in the warrant, and law enforcement may need to conduct more extensive searches to locate

---

investigative agent is a trained computer forensic examiner, it is not always necessary to separate these duties. Computer forensic examiners often work closely with investigative personnel to assist investigators in their search for digital evidence. Computer forensic examiners are needed because they generally have technological expertise that investigative agents do not possess. Computer forensic examiners, however, often lack the factual and investigative expertise that an investigative agent may possess on any given case. Therefore, it is often important that computer forensic examiners and investigative personnel work closely together.

UNITED STATES ATTORNEY
700 STEWART ST, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

evidence that falls within the scope of the warrant. The search techniques that will be used will be only those methodologies, techniques and protocols as may reasonably be expected to find, identify, segregate and/or duplicate the items authorized to be seized pursuant to Attachment B to this affidavit. Those techniques, however, may necessarily expose many or all parts of a hard drive to human inspection in order to determine whether it contains evidence described by the warrant.

b. Agents may utilize hash values to exclude certain known files, such as the operating system and other routine software, from the search results. However, because the evidence I am seeking does not have particular known hash values, agents will not be able to use any type of hash value library to locate the items identified in Attachment B.

APPLE DEVICE TOUCH ID

58. As described above, IRS records show that at least one Apple iPhone and one Apple laptop have accessed IRS websites using the Zhang IP address registered to the SUBJECT PREMISES for information relevant to the above-described scheme during the relevant time period. Based on this, I believe it is likely that the SUBJECT PREMISES will contain at least one Apple brand device, such as an iPhone.

59. I know from my training and experience, as well as from information found in publicly available materials including those published by Apple, that some models of Apple devices such as iPhones and iPads offer their users the ability to unlock the device via the use of a fingerprint or thumbprint (collectively, "fingerprint") in lieu of a numeric or alphanumeric passcode or password. This feature is called Touch ID.

60. If a user enables Touch ID on a given Apple device, he or she can register up to 5 fingerprints that can be used to unlock that device. The user can then use any of the registered fingerprints to unlock the device by pressing the relevant finger(s) to the device's Touch ID sensor, which is found in the round button (often referred to as the "home" button) found at the bottom center of the front of the device. In my training and experience, users of Apple devices that offer Touch ID often enable it because it is considered to be a more convenient way to unlock the device than by entering a numeric or alphanumeric passcode or password, as well as a more secure way to protect the device's contents. This

UNITED STATES ATTORNEY
700 STEWART ST, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

is particularly true when the user(s) of the device are engaged in criminal activities and thus have a heightened concern about securing the contents of the device.

61. In some circumstances, a fingerprint cannot be used to unlock a device that has Touch ID enabled, and a passcode or password must be used instead. These circumstances include: (1) when more than 48 hours has passed since the last time the device was unlocked and (2) when the device has not been unlocked via Touch ID in 8 hours and the passcode or password has not been entered in the last 6 days. Thus, in the event law enforcement encounters a locked Apple device, the opportunity to unlock the device via Touch ID exists only for a short time. Touch ID also will not work to unlock the device if (1) the device has been turned off or restarted; (2) the device has received a remote lock command; and (3) five unsuccessful attempts to unlock the device via Touch ID are made.

62. The passcode or password that would unlock the Apple device(s) found during the search of the SUBJECT PREMISES is not known to law enforcement. Thus, it will likely be necessary to press the finger(s) of the user(s) of the Apple device(s) found during the search of the SUBJECT PREMISES to the device's Touch ID sensor in an attempt to unlock the device for the purpose of executing the search authorized by this warrant. Attempting to unlock the relevant Apple device(s) via Touch ID with the use of the fingerprints of the user(s) is necessary because the government may not otherwise be able to access the data contained on those devices for the purpose of executing the search authorized by this warrant.

63. In my training and experience, the person who is in possession of a device or has the device among his or her belongings at the time the device is found is likely a user of the device. However, in my training and experience, that person may not be the only user of the device whose fingerprints are among those that will unlock the device via Touch ID, and it is also possible that the person in whose possession the device is found is not actually a user of that device at all. Furthermore, in my training and experience, I know that in some cases it may not be possible to know with certainty who is the user of a given

UNITED STATES ATTORNEY
700 STEWART ST, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

device, such as if the device is found in a common area of a premises without any identifying information on the exterior of the device. Thus, it will likely be necessary for law enforcement to have the ability to require any occupant of the SUBJECT PREMISES to press their finger(s) against the Touch ID sensor of the locked Apple device(s) found during the search of the SUBJECT PREMISES in order to attempt to identify the device's user(s) and unlock the device(s) via Touch ID.

64. Although I do not know which of a given user's 10 fingerprints is capable of unlocking a particular device, based on my training and experience I know that it is common for a user to unlock a Touch ID-enabled Apple device via the fingerprints on thumbs or index fingers. In the event that law enforcement is unable to unlock the Apple device(s) found in the SUBJECT PREMISES as described above within the five attempts permitted by Touch ID, this will simply result in the device requiring the entry of a password or passcode before it can be unlocked.

65. Due to the foregoing, I request that the Court authorize law enforcement to press the fingers (including thumbs) of individuals found at the SUBJECT PREMISES to the Touch ID sensor of the Apple brand device(s), such as an iPhone or iPad, found at the SUBJECT PREMISES for the purpose of attempting to unlock the device via Touch ID in order to search the contents as authorized by this warrant.

//

//

UNITED STATES ATTORNEY
700 STEWART ST, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

CONCLUSION

66. Based on the foregoing, I believe there is probable cause that evidence, fruits, and instrumentalities of violations of 18 U.S.C. § 1343 (Wire Fraud), 18 U.S.C. § 1344 (Bank Fraud), 18 U.S.C. § 1014 (False Statements to a Financial Institution), and 15 U.S.C. § 645(a) (False Statements to the Small Business Administration) are located at the SUBJECT PREMISES, as more fully described in Attachment A to this Affidavit, as well as on and in any digital devices or other electronic storage media found at the SUBJECT PREMISES. Specifically, the SUBJECT PREMISES was used as the business location address for sham entities used to fraudulently apply for PPP loans. There is probable cause to believe, therefore, that the SUBJECT PREMISES will contain records showing when the entities were created and how they were used. In addition, as described above, false and falsified digital records were submitted in support of fraudulent PPP loan applications using an IP address registered to the SUBJECT PREMISES. There is probable cause to believe, therefore, that the SUBJECT PREMISES will contain digital devices that were used to carry out the fraud scheme and contain evidence of it.

67. I therefore request that the court issue a warrant authorizing a search of the SUBJECT PREMISES, as well as any digital devices and electronic storage media located therein, for the items more fully described in Attachment B hereto, incorporated herein by reference, and the seizure of any such items found therein.

Cole Ashcraft

Cole Ashcraft, Affiant
Special Agent, TIGTA

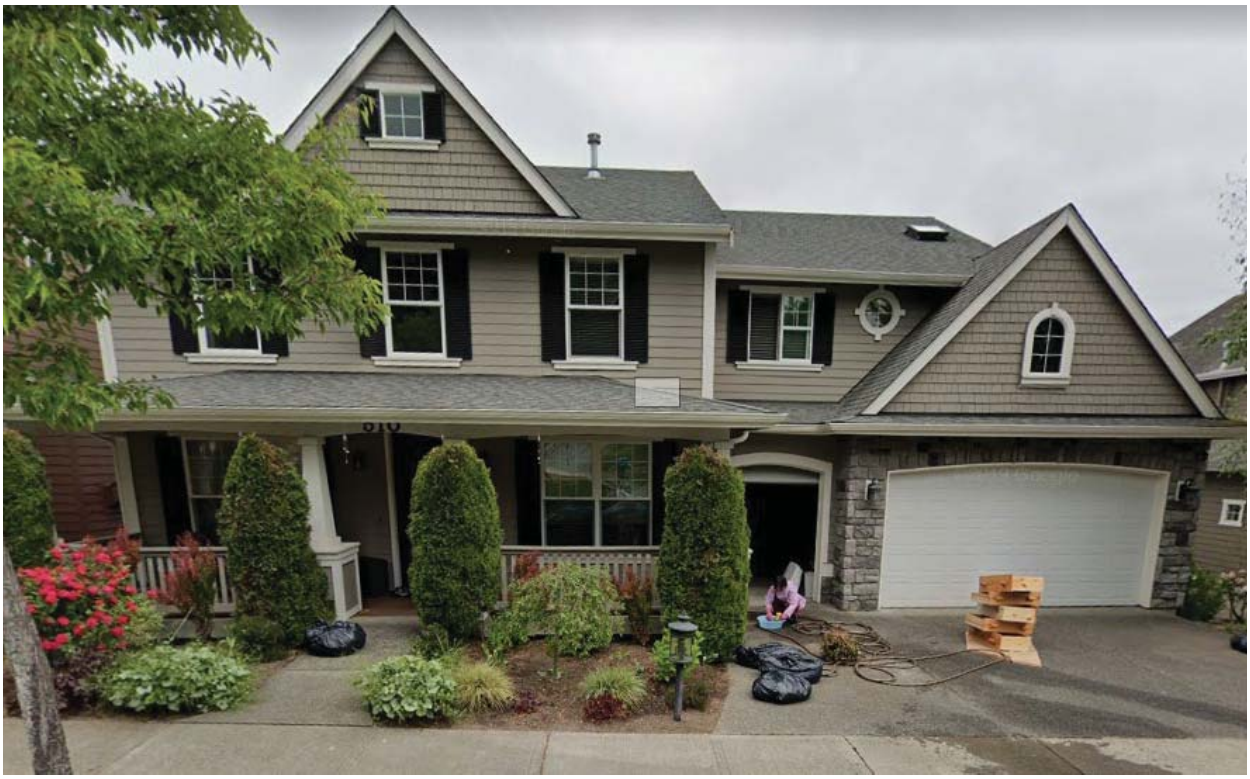
The above-named agent provided a sworn statement attesting to the truth of the contents of the foregoing affidavit on the 21st day of May, 2020.

MARY ALICE THEILER
United States Magistrate Judge

UNITED STATES ATTORNEY
700 STEWART ST, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

ATTACHMENT A

The property to be searched is 510 Sky Country Way NW, Issaquah, Washington 98027, further described as a beige single-family home with an attached garage, front porch, grey roof, and shingled siding, and any digital device/s or other electronic storage media found therein. The property to be searched is pictured below:



.

UNITED STATES ATTORNEY
700 STEWART ST, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

ATTACHMENT B

ITEMS TO BE SEIZED

The following records, documents, files, or materials, in whatever form, including handmade or mechanical form (such as printed, written, handwritten, or typed); photocopies or other photographic form; and electrical, electronic, and magnetic form (such as tapes, cassettes, hard disks, floppy disks, diskettes, compact discs, CD-ROMs, DVDs, optical discs, Zip cartridges, printer buffers, smart cards, or electronic notebooks, or any other electronic storage medium) that constitute evidence, instrumentalities, or fruits of violations of 18 U.S.C. § 1343 (Wire Fraud), 18 U.S.C. § 1344 (Bank Fraud), 18 U.S.C. § 1014 (False Statements to a Financial Institution), and 15 U.S.C. § 645(a) (False Statements to the Small Business Administration):

1. All records relating to violations of 18 U.S.C. § 1343 (Wire Fraud), 18 U.S.C. § 1344 (Bank Fraud), 18 U.S.C. § 1014 (False Statements to a Financial Institution), and 15 U.S.C. § 645(a) (False Statements to the Small Business Administration) and involving Baoke Zhang since in or about April 2020 including:

a. any information relating to the Paycheck Protection Program;

b. any information relating to the U.S. Small Business Administration;

c. any tax records and information relating to the Internal Revenue Service;

d. any information relating to any lender that is approved by the U.S. Small Business Administration to accept applications under the CARES ACT;

e. any information relating to Baoke Zhang dba Baoke Zhang;

f. any information relating to Cloud Optimization LLC;

g. any information identifying the individual or individuals that committed the above-described offenses; and

h. any information relating to any personal identifying information associated with any names provided in support of PPP loan applications as employees of

UNITED STATES ATTORNEY
700 STEWART ST, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

Baoke Zhang dba Baoke Zhang, Cloud Optimization LLC, or any other entity controlled, created, or operated by Baoke Zhang;

2. Digital devices[2] or other electronic storage media[3] and/or their components, which include:

a. Any digital device or other electronic storage media capable of being used to commit, further, or store evidence of the offenses listed above;

b. Any digital devices or other electronic storage media used to facilitate the transmission, creation, display, encoding or storage of data, including word processing equipment, modems, docking stations, monitors, cameras, printers, plotters, encryption devices, and optical scanners;

c. Any magnetic, electronic or optical storage device capable of storing data, such as floppy disks, hard disks, tapes, CD-ROMs, CD-R, CD-RWs, DVDs, optical disks, printer or memory buffers, smart cards, PC cards, memory calculators, electronic dialers, electronic notebooks, and personal digital assistants;

d. Any documentation, operating logs and reference manuals regarding the operation of the digital device or other electronic storage media or software;

e. Any applications, utility programs, compilers, interpreters, and other software used to facilitate direct or indirect communication with the computer hardware, storage devices, or data to be searched;

---

[2] "Digital device" includes any device capable of processing and/or storing data in electronic form, including, but not limited to: central processing units, laptop, desktop, notebook or tablet computers, computer servers, peripheral input/output devices such as keyboards, printers, scanners, plotters, monitors, and drives intended for removable media, related communications devices such as modems, routers and switches, and electronic/digital security devices, wireless communication devices such as mobile or cellular telephones and telephone paging devices, personal data assistants ("PDAs"), iPods/iPads, Blackberries, digital cameras, digital gaming devices, global positioning satellite devices (GPS), or portable media players.

[3] Electronic Storage media is any physical object upon which electronically stored information can be recorded. Examples include hard disks, RAM, floppy disks, flash memory, CD-ROMs, and other magnetic or optical media.

UNITED STATES ATTORNEY
700 STEWART ST, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

f. Any physical keys, encryption devices, dongles and similar physical items that are necessary to gain access to the computer equipment, storage devices or data; and

g. Any passwords, password files, test keys, encryption codes or other information necessary to access the computer equipment, storage devices or data.

3. For any digital device or other electronic storage media upon which electronically stored information that is called for by this warrant may be contained, or that may contain things otherwise called for by this warrant:

a. evidence of who used, owned, or controlled the digital device or other electronic storage media at the time the things described in this warrant were created, edited, or deleted, such as logs, registry entries, configuration files, saved usernames and passwords, documents, browsing history, user profiles, email, email contacts, "chat," instant messaging logs, photographs, and correspondence;

b. evidence of software that would allow others to control the digital device or other electronic storage media, such as viruses, Trojan horses, and other forms of malicious software, as well as evidence of the presence or absence of security software designed to detect malicious software;

c. evidence of the lack of such malicious software;

d. evidence of the attachment to the digital device of other storage devices or similar containers for electronic evidence;

e. evidence of counter-forensic programs (and associated data) that are designed to eliminate data from the digital device or other electronic storage media;

f. evidence of the times the digital device or other electronic storage media was used;

g. passwords, encryption keys, and other access devices that may be necessary to access the digital device or other electronic storage media;

h. documentation and manuals that may be necessary to access the digital device or other electronic storage media or to conduct a forensic examination of the digital device or other electronic storage media;

i. contextual information necessary to understand the evidence described in this attachment.

UNITED STATES ATTORNEY
700 STEWART ST, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

4. Records and things evidencing the use of Internet Protocol address 24.22.166.81 to communicate with servers controlled or used by the IRS, Ready Capital and any associated entities, PayPal, Inc., and any associated entities, and WebBank and any associated entities including:

a. routers, modems, and network equipment used to connect computers to the Internet;

b. records of Internet Protocol addresses used;

c. records of Internet activity, including firewall logs, caches, browser history and cookies, "bookmarked" or "favorite" web pages, search terms that the user entered into any Internet search engine, and records of user-typed web addresses.

During the execution of the search of the SUBJECT PREMISES described in Attachment A, law enforcement personnel are authorized to press the fingers (including thumbs) of individuals found at the SUBJECT PREMISES to the Touch ID sensor of the Apple brand device(s), such as an iPhone or iPad, found at the SUBJECT PREMISES for the purpose of attempting to unlock the device via Touch ID in order to search the contents as authorized by this warrant.

THE SEIZURE OF DIGITAL DEVICES OR OTHER ELECTRONIC STORAGE MEDIA AND/OR THEIR COMPONENTS AS SET FORTH HEREIN IS SPECIFICALLY AUTHORIZED BY THIS SEARCH WARRANT, NOT ONLY TO THE EXTENT THAT SUCH DIGITAL DEVICES OR OTHER ELECTRONIC STORAGE MEDIA CONSTITUTE INSTRUMENTALITIES OF THE CRIMINAL ACTIVITY DESCRIBED ABOVE, BUT ALSO FOR THE PURPOSE OF THE CONDUCTING OFF-SITE EXAMINATIONS OF THEIR CONTENTS FOR EVIDENCE, INSTRUMENTALITIES, OR FRUITS OF THE AFOREMENTIONED CRIMES

UNITED STATES ATTORNEY
700 STEWART ST, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970